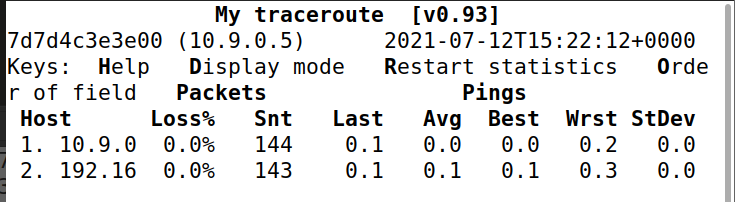
**网安实训实验报告3**

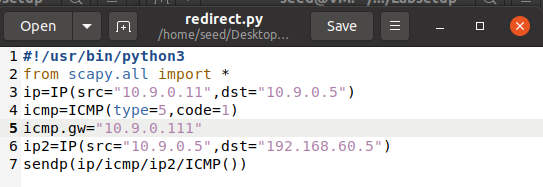
**57118139顾宸玮**

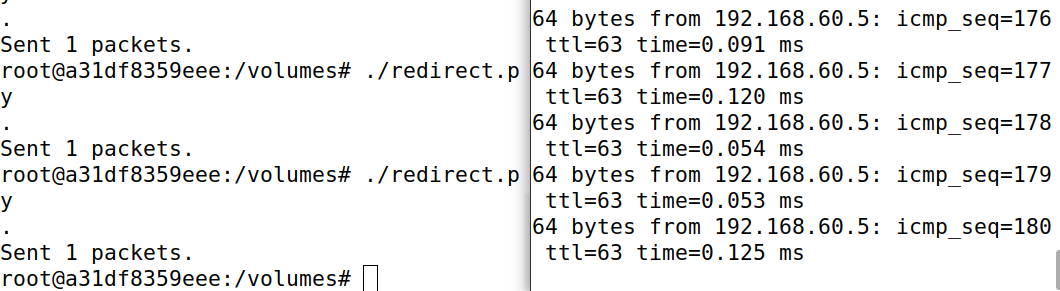
**Task 1: Launching ICMP Redirect Attack**

首先在未攻击前查看victim traceroute到192.168.60.5，可以发现就两个host

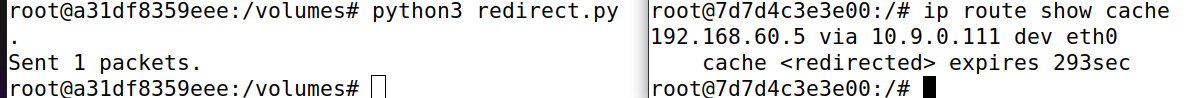


将py文件补充完整，进行攻击：

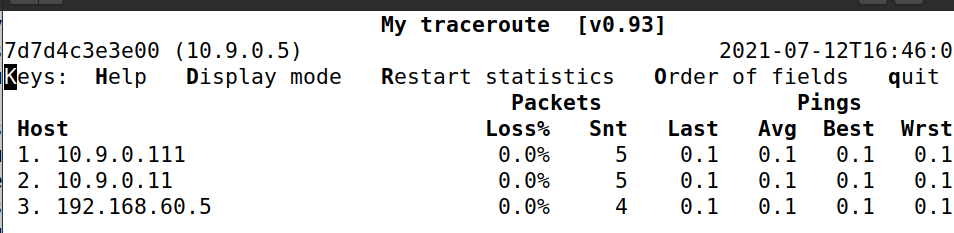




可以发现，查看victim的cache发现被重定向了

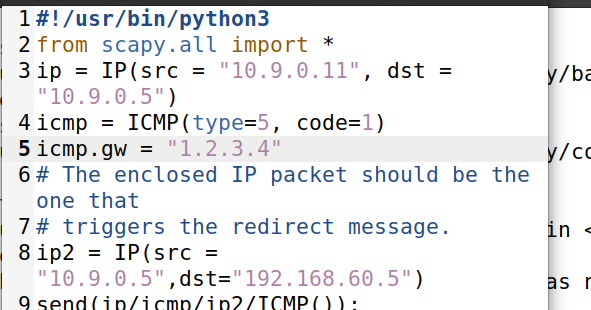


再次 mtr -n 192.168.60.5可以发现多了一条host



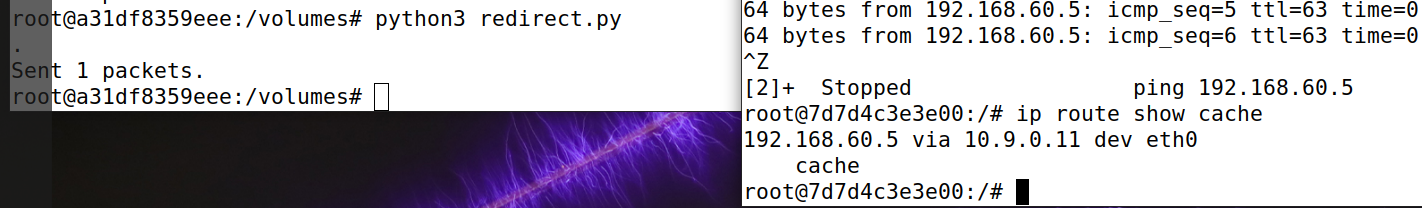
**Question 1: Can you use ICMP redirect attacks to redirect to a remote machine? Namely, the IP address assigned to icmp.gw is a computer not on the local LAN. Please show your experiment result, and explain your observation.**

将icmp.gw改成外网网关



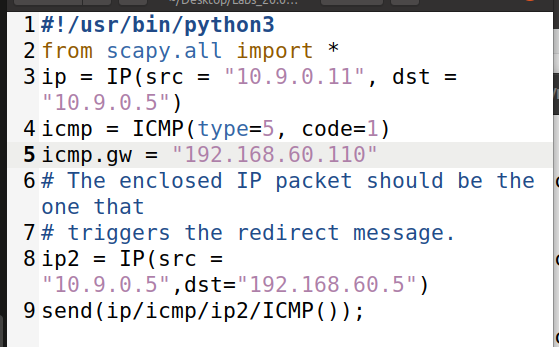


将cache清空后发现并没有被重定向

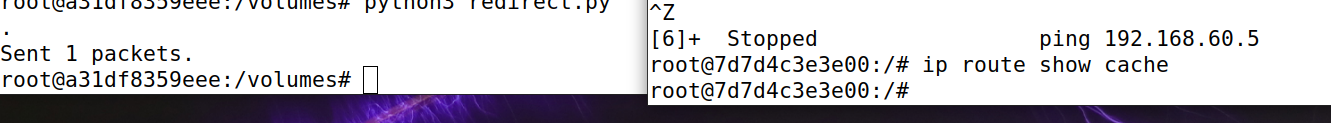


**Question 2: Can you use ICMP redirect attacks to redirect to a non-existing machine on the samenet work? Namely, the IP address assigned to icmp.gw is a local computer that is either offline or non-existing. Please show your experiment result, and explain your observation.**

将icmp.gw改成内网不存在地址

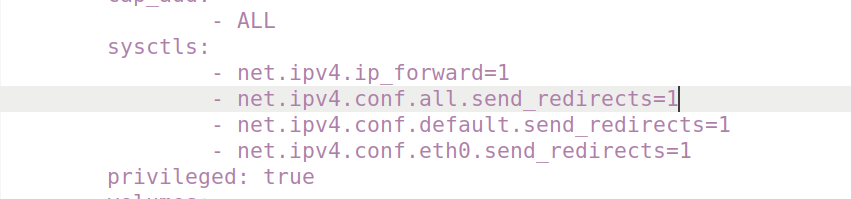


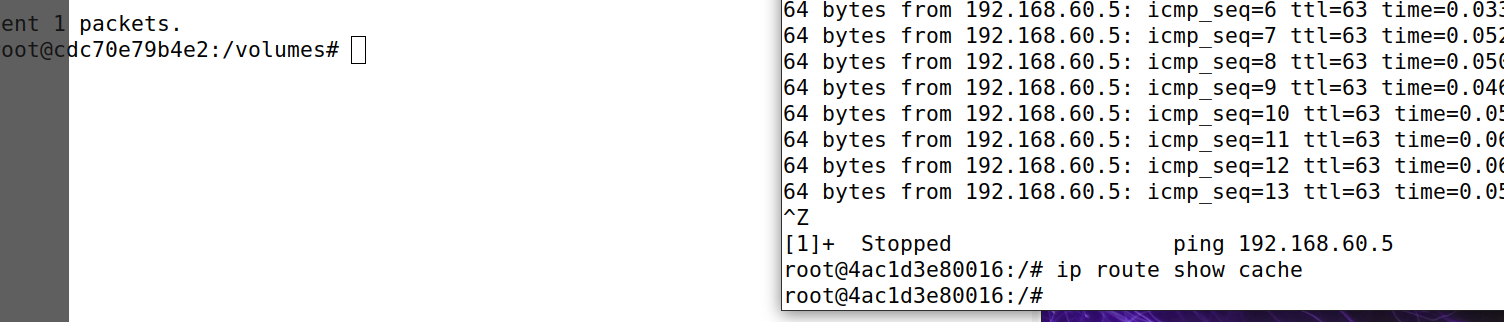
发现并没有被重定向



**Question 3: If you look at the docker-compose.yml file, you will find the following entries for the malicious router container. What are the purposes of these entries? Please change their value to 1, and launch the attack again. Please describe and explain your observation.**

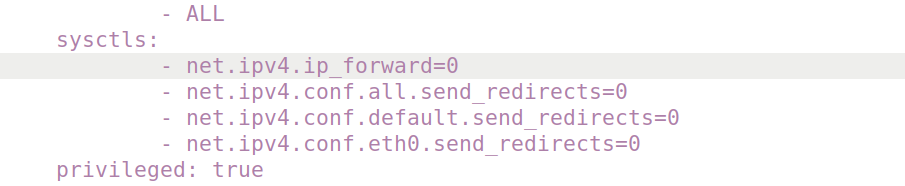
将以下值置1，可以发现攻击没有效果了，以下几项表示是否转发重定向ipv4包，即是否会随便改变路由。



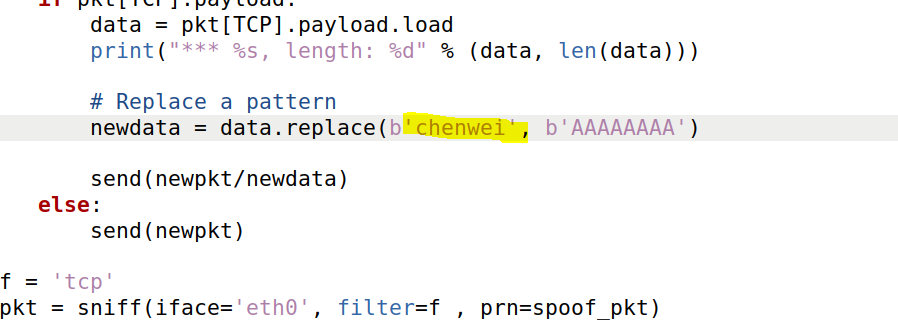


**Task 2: Launching the MITM Attack**

首先把恶意路由的转发关掉



把代码中的替换文字改成我的名字“chenwei”

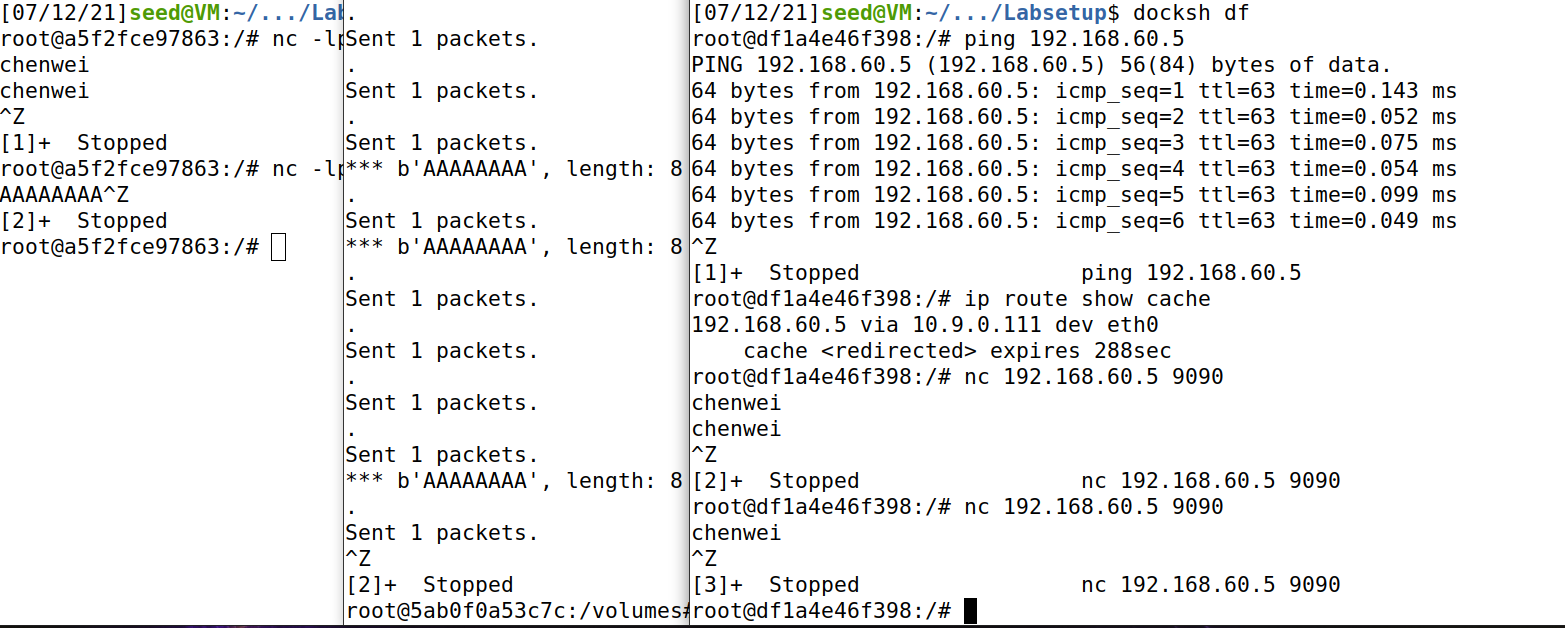


该恶意程序捕获的是从victim发到192.168.60.5方向上的包，因为在victim中输入的数据最终被转发到192.168.60.5上

**Question 4: In your MITM program, you only need to capture the traffifics in one direction. Please indicate which direction, and explain why**

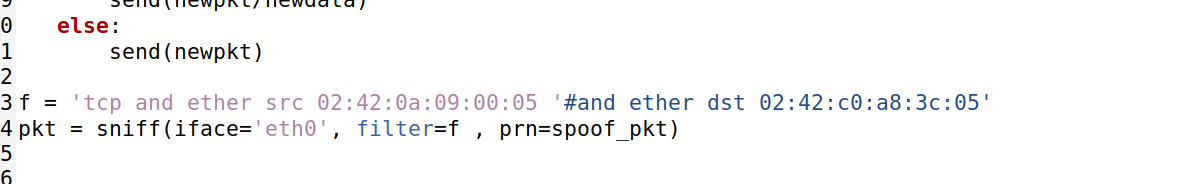
首先再做一次第一问，重定向路由

在恶意路由上运行程序，在victim上连接192.168.60.5，发送报文“chenwei”，可以发现被替换成”AAAAAAAA”

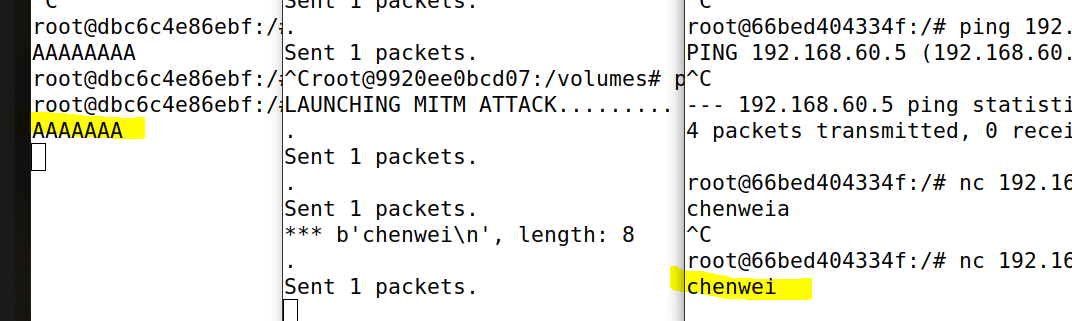


**Question 5: In the MITM program, when you capture the nc traffifics from A (10.9.0.5), you can use A’s IP address or MAC address in the fifilter. One of the choices is not good and is going to create issues, even though both choices may work. Please try both, and use your experiment results to show which choice is the correct one, and please explain your conclusion.**

将filter改成victim的MAC地址



可以发现恶意路由运行时发的包减少，并且不会接收自己发送的包



**感想：**

这次实验主要体验了ICMP重定向的操作，实验中遇到了很多困难，特别是在最后一个实验中，一开始将替换的字符串由8个改成7个（因为“chenwei”是7个），测试操作后，发现恶意路由只是在重复我在victim上发的包，并没有在192.168.60.5上显示出来，后来重复修改A的数量，才能够正确输出。总而言之，对于ICMP重定向攻击这个攻击手段有了更深的理解。